
# NATO and National Responses to Hostile Influence

Elīna Lange-Ionatamišvili

# NATO ACT Strategic Foresight Analysis (2017)

There has been a serious breakdown in security both regionally and within states in recent years.

*(...Russia's annexation of Crimea & intervention in eastern Ukraine...)*

These developments highlight the evolution of **hybrid warfare**, where an adversary's use of **unattributable means** and **plausible deniability** signals a paradigm shift in the use of power.

# Hybrid threats

Hybrid threats are methods and activities that are targeted towards vulnerabilities of the opponent. Vulnerabilities can be created by **historical memory**, legislation, old practices, geostrategic factors, **strong polarisation of society**, technological disadvantages or **ideological differences**.

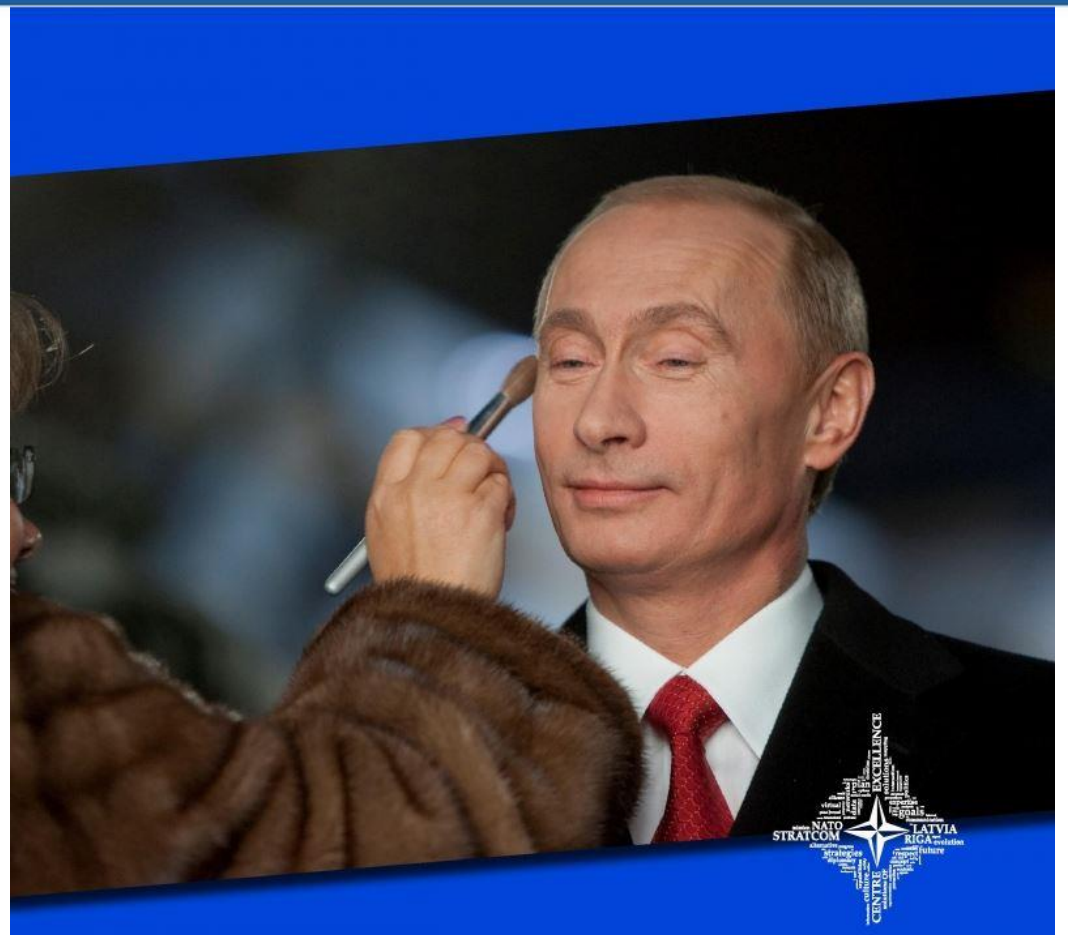
Hybrid CoE

The European Centre of Excellence for Countering Hybrid Threats

# Attack on democratic processes and values

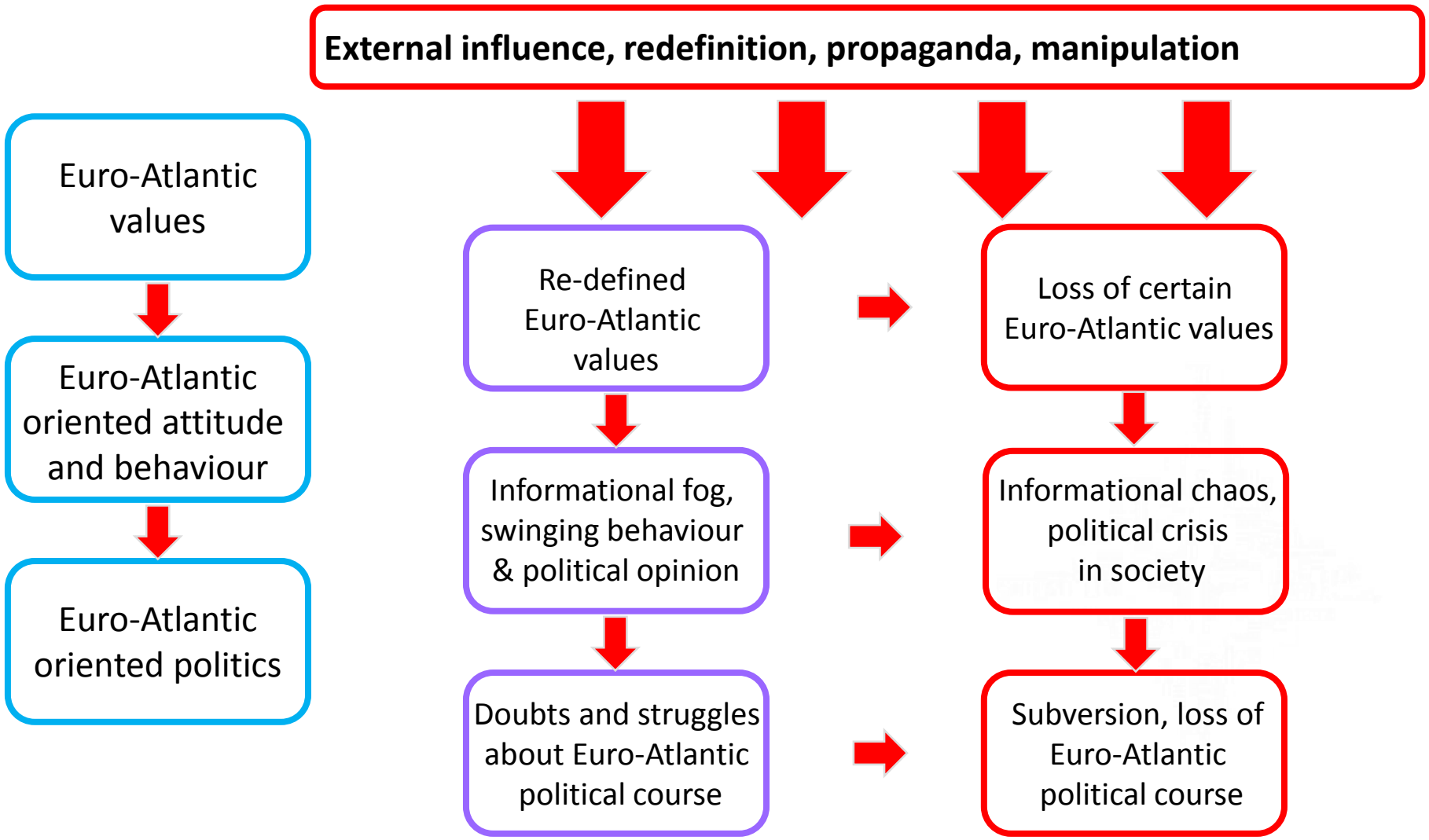
## Russian disinformation distorts American and European democracy

*The Mueller indictment reveals some of the Kremlin's tactics*

REDEFINING EURO-ATLANTIC VALUES:
RUSSIA`S MANIPULATIVE TECHNIQUES

# Correlation between values, public opinion and politics



# Unattributable, plausible deniability....

Russia's strategy of information warfare, the role of proxies in undermining attribution efforts, and blunt lies from highest country officials, consequentially hamper «victims'» political will to recognise provocations as such and respond to them.

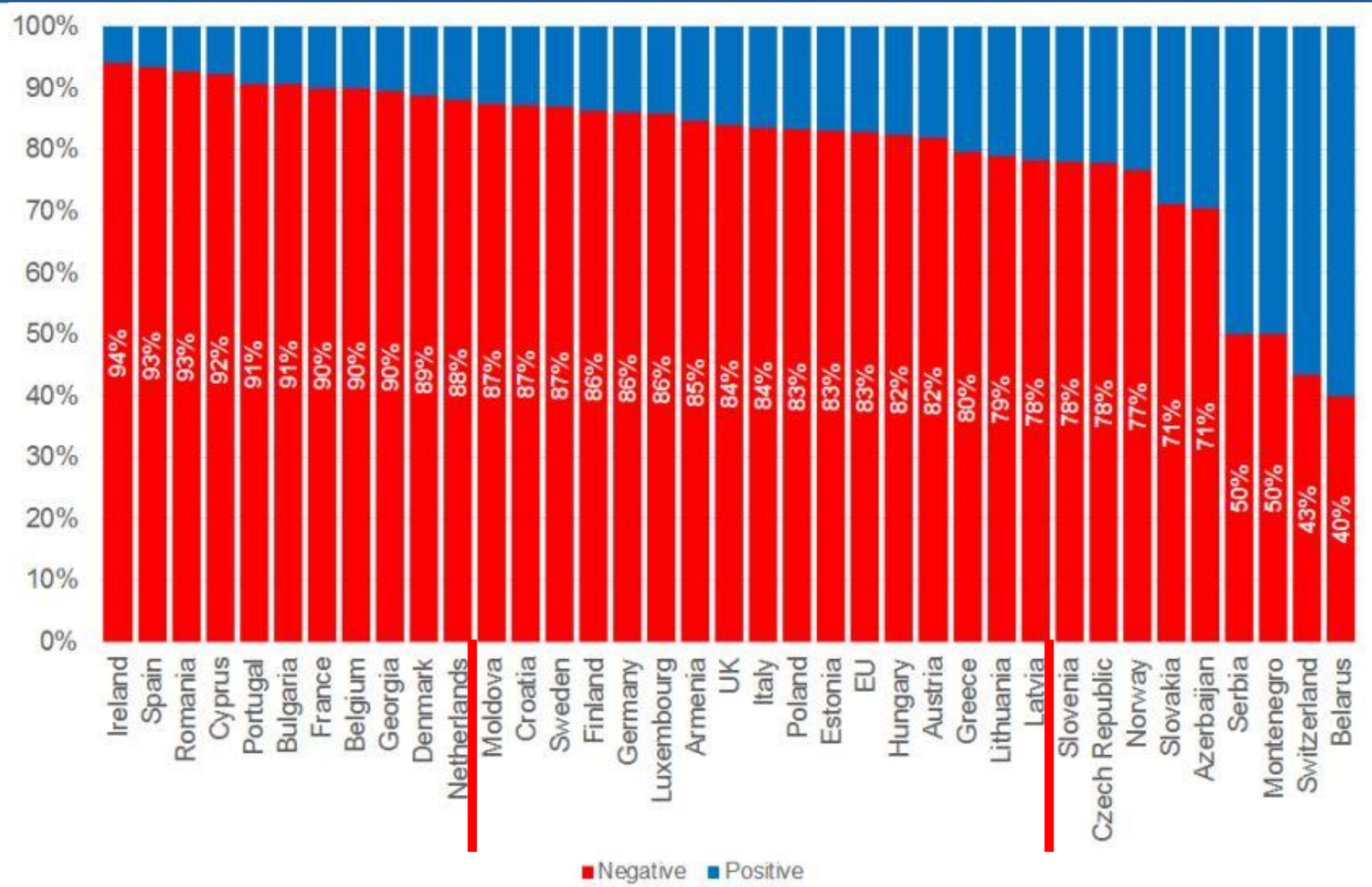
# French Presidential Election of 2017



- Investigative reporters: Bellingcat, NYT, WP, CNN...
- French TV5 (2015)
- German Parliament (2014)
- International banking institutions (2015)
- World Anti-Doping Agency (2016)
- Dutch Safety Board (2015)
- Democratic National Committee (2016)
- Dutch ministries (2017)
- Angela Merkel Campaign (2017)
- International Olympic Committee (2018)


LIVE House of Commons
BREAKING NEWS
UK RUSSIA MEASURES
May: It's essential we stand up with our allies for our values
BBC NEWS 12:43 IS TO SHUT ALL 100 OF ITS UK STORES, RESULTING IN LO

# Maintaining support of Russian audience



# Our Project on Countering Hostile Influence

- Provide an understanding of how influence works across the spectrum of national power dimensions (DIME+ Financial, Intelligence, Legal)

- Particular focus is on Russia

- Ambiguity is the buzzword

# Thematic areas of threat

- GONGOs
- NGOs
- Academic Groups
- Lawfare
- Cyber operations
- Religious groups
- Territorial violations
- Agitation and civil unrest
- Coercion through threat of use of force
- Media
- Espionage and infiltration
- Economic leverage
- Energy dependency
- Bribery and corruption
- Exploitation of ethnic and cultural identities
- Political actors

# The Database


# 012 Cyber-Attacks on Estonia

Russia × Estonia ×

Cyber Operations ×

**Summary** | Context | Measures | Security Interests | Narratives | Conclusions

Normal

## SUMMARY

In April and May 2007, Estonia was the target of a coordinated cyber attack. Over a three-week period, government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all targeted, predominantly by a Distributed Denial of Service (DDoS). The cyber attack coincided with the Estonian government's decision to relocate the 'Bronze Soldier Memorial' in Tallinn, leading to significant civil disturbance in both Estonia and Russia.

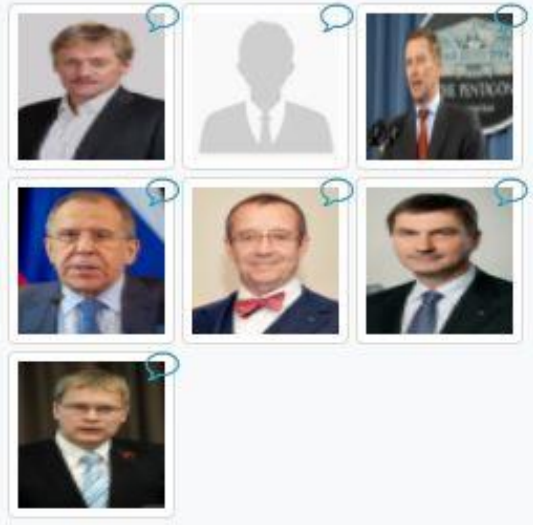
The vast majority of malicious network traffic was of Russian-language origin and had indications of political motivation. The Russian government denied any involvement; however, the cyber attacks were accompanied by hostile political rhetoric by Russian officials, unfriendly economic measures, and refusal to cooperate with the Estonian investigation in the aftermath of the attacks, which likely encouraged the perpetrators.

The attacks caused some disruption and economic cost to Estonia. Perhaps more importantly, though, they exposed Estonia's vulnerabilities, and demonstrated the *potential* of cyber attacks to cause far more lasting damage if intended. However, the incident also demonstrated Estonia's capabilities and resilience in countering the cyber attacks. Ultimately, the shock caused by the cyber attack led to a significant strengthening of cyber defence capabilities, institutions and legislation in Estonia, the European Union, and NATO.

Export Case Study

Word Document , PDF

Actors (7) edit



Events (15) edit

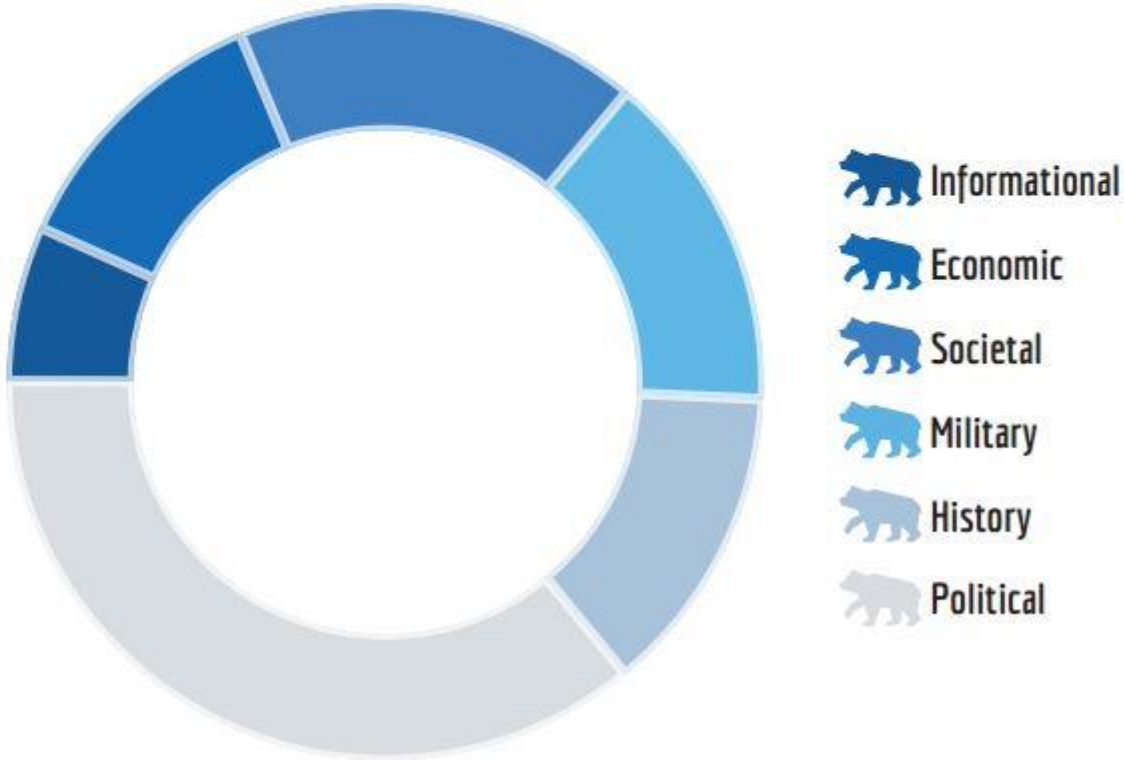
Timeline Show/Hide

- May 09, 2006 Estonia's national Comp...
- Apr 27, 2007 26- Excavation works beg...
- Apr 27, 2007 First wave of cyber-attack...
- Apr 28, 2007 Co-ordinated fight-back ...
- May 04, 2007 Second and better-orga...
- May 09, 2007 Peak in the attacks, coinc...
- May 19, 2007 Cyber-attacks abruptly a...
- Sep 01, 2007 Proposition of a "Cyber D...

# Our Project on Mapping Hostile Narratives

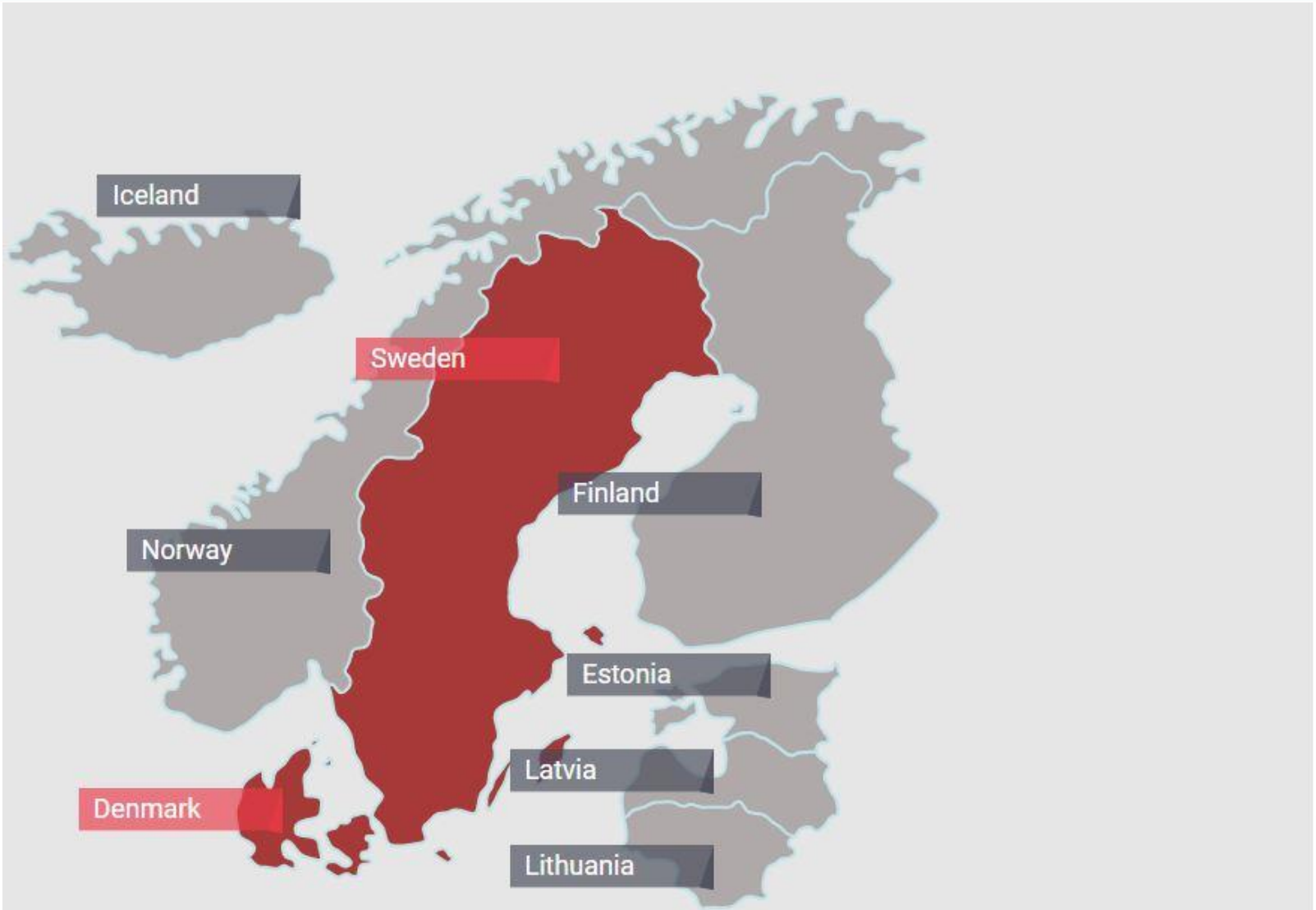
## Dimensions

Proportional presence of national power dimensions in the information environment of the Nordic–Baltic region.



# Our Project on Mapping Hostile Narratives

# Our Project on Mapping Hostile Narratives




BACK TO FILTER

- Refugee criris in the EU is out of control
- Refugees and migrants as a destabilising factor
- EU will break up eventually
- Support to nationalist, far-right, secessionist movements
- Magnified threat of nationalist and far-right movements in Europe
- NATO is obsolete
- If FL & SE join NATO, RU will act
- Radical Islam as a destabilizing factor.
- The "Russian threat" is a made up threat on the domestic agenda
- Sweden is delusional in its fear of "Russian meddling" in upcoming elections

# Recommendations

- Call it out and be ready to respond
- Stop mirroring
- Threat awareness and quick adaptability are key. (Public reporting of intelligence findings )
- A diverse, visible response by Government/Parliament helps raise awareness of the threat and can act as a deterrent
- Consolidate and enhance Cyber Security & Cyber Defences
- Encourage vigilance and cooperation of Non-Government Actors, Media, Private Sector
- Balance disincentivising the sharing of disinformation with freedom of expression concerns
- Follow the money & expose it. (Take action against money loundering)


# Thank you!

elina.lange@stratcomcoe.org